日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２０００年１１月１６日

出願番号
Application Number: 特願２０００－３５０１８５

出願人
Applicant(s): 富士ゼロックス株式会社

２００１年１２月　７日

特許庁長官
Commissioner,
Japan Patent Office 及川耕造

出証番号　出証特２００１－３１０６８４３

【書類名】　特許願
【整理番号】　FE00-01400
【提出日】　平成12年11月16日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 17/60
【発明の名称】　個人証明書サブジェクト名処理装置および方法
【請求項の数】　9
【発明者】
【住所又は居所】　神奈川県川崎市高津区坂戸３丁目２番１号　ＫＳＰ　Ｒ＆Ｄ　ビジネスパークビル　富士ゼロックス株式会社内
【氏名】　稲田　龍
【発明者】
【住所又は居所】　神奈川県川崎市高津区坂戸３丁目２番１号　ＫＳＰ　Ｒ＆Ｄ　ビジネスパークビル　富士ゼロックス株式会社内
【氏名】　黒崎　雅人
【特許出願人】
【識別番号】　000005496
【氏名又は名称】　富士ゼロックス株式会社
【電話番号】　0462-38-8516
【代理人】
【識別番号】　100086531
【弁理士】
【氏名又は名称】　澤田　俊夫
【電話番号】　03-5541-7577
【選任した代理人】
【識別番号】　100093241
【弁理士】
【氏名又は名称】　宮田　正昭

【選任した代理人】

【識別番号】　100101801

【弁理士】

【氏名又は名称】　山田　英治

【手数料の表示】

【予納台帳番号】　038818

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　個人証明書サブジェクト名処理装置および方法

【特許請求の範囲】

【請求項１】　サブジェクト名の所定のエレメントが保持者の所属組織および個人ＩＤ以外の属性を表す個人証明書を受信して当該サブジェクト名を処理する個人証明書サブジェクト名処理装置において、

上記個人証明書を受信する手段と、

受信した個人証明書に含まれるサブジェクト名の階層中の所定のエレメントを抽出する手段と、

上記所定のエレメントの値が表す、保持者の所属組織および個人ＩＤ以外の属性に基づいて、アクセス権限を決定する手段とを有することを特徴とする個人証明書サブジェクト名処理装置。

【請求項２】　上記サブジェクト名の所定階層のオーガニゼーショナル・ユニット・ネームが、保持者がオーガニゼーション・ネームが表す組織の構成員ではなく、かつ当該組織に対して協力していることを示す請求項１記載の個人証明書サブジェクト名処置装置。

【請求項３】　上記サブジェクト名の所定階層のオーガニゼーショナル・ユニット・ネームが、保持者が参加するプロジェクト名を表す請求項１または２記載の個人証明書サブジェクト名処理装置。

【請求項４】　上記サブジェクト名の所定階層のオーガニゼーショナル・ユニット・ネームが、オーガニゼーション・ネームが表す組織に対して協力し、かつ保持者が属する、協力組織名を表す請求項１、２または３記載の個人証明書サブジェクト名処理装置。

【請求項５】　上記サブジェクト名の所定階層のオーガニゼーショナル・ユニット・ネームが、保持者が参加する業務の種類を表す請求項１、２、３または４記載の個人証明書サブジェクト名処理装置。

【請求項６】　上記サブジェクト名のコモンネームが、保持者が参加する業目うの種類を表す請求項１、２、３または４記載の個人証明書サブジェクト名処理装置。

【請求項７】　個人証明書を受信する手段と、

受信した個人証明書に含まれるサブジェクト名の階層中の所定のエレメントを抽出する手段と、

上記所定のエレメントの値に基づいてアクセス権限を決定する手段とを有することを特徴とする個人証明書サブジェクト名処理装置。

【請求項８】　サブジェクト名の所定のエレメントが保持者の所属組織および個人ＩＤ以外の属性を表す個人証明書を受信して当該サブジェクト名を処理する個人証明書サブジェクト名処理方法において、

上記個人証明書を受信するステップと、

受信した個人証明書に含まれるサブジェクト名の階層中の所定のエレメントを抽出するステップと、

上記所定のエレメントの値が表す、保持者の所属組織および個人ＩＤ以外の属性に基づいて、アクセス権限を決定するステップとを有することを特徴とする個人証明書サブジェクト名処理方法。

【請求項９】　サブジェクト名のオーガニゼーショナル・ユニット・ネームおよびコモン・ネームの少なくとも１つが保持者の所属組織および個人ＩＤ以外の属性を表す個人証明書を記録したコンピュータ読取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

この発明は、個人証明書のサブジェクト名を利用してアクセスを制御する技術に関する。

【０００２】

【従来の技術】

ＩＴＵ－Ｔ勧告Ｘ．５０９はディレクトリモデル認証を規定しており、このディレクトリモデル認証に準拠して個人証明書を発行局（認証局）から発行してもらう。発行局は申請人から証明書の発行に必要な情報（名前、所属、公開鍵等）を受け取り所定のポリシーに従い証明書を発行し、証明書を所定の証明書格納部に保存する。申請人は証明書格納部から証明書を取り出すことができる。

【０００３】

ところで、個人証明書のサブジェクト名を見ただけでは、その証明書の保持者がどういう権限を有しており、どういう性質をもっているか不明である。保持者が有している権限や性質を知るために種々のアプローチが採用されている。例えば、証明書のサブジェクト名と権限とをデータベースに登録し、証明書を用いたアクセスがあるたびにデータベースに問合せる。しかしこの方法は効率の面で問題があった。

【０００４】

【発明が解決する課題】

この発明は、以上の事情を考慮してなされたものであり、証明書のサブジェクト名から直ちにその権限や性質を知ることができ、これを用いて簡易にアクセス制御等を行える技術を提供することを目的としている。

【０００５】

【課題を解決するための手段】

この発明によれば、上述の目的を達成するために、特許請求の範囲に記載のとおりの構成を採用している。ここでは、発明を詳細に説明するのに先だって特許請求の範囲の記載について補充的に説明を行っておく。

【０００６】

この発明の一側面によれば、上述の目的を達成するために、サブジェクト名の所定のエレメントが保持者の所属組織および個人ＩＤ以外の属性を表す個人証明書を受信して当該サブジェクト名を処理する個人証明書サブジェクト名処理装置に：上記個人証明書を受信する手段と；受信した個人証明書に含まれるサブジェクト名の階層中の所定のエレメントを抽出する手段と；上記所定のエレメントの値が表す、保持者の所属組織および個人ＩＤ以外の属性に基づいて、アクセス権限を決定する手段とを設けるようにしている。

【０００７】

この構成においては、個人証明書に含まれるサブジェクト名の記載内容に基づいて、権限や性質に応じたアクセス制御を行うことができる。

【０００８】

なお、この発明は装置やシステムとして実現できるのみでなく、方法としても実現できる。またこのような方法の一部をコンピュータプログラムとして実現してもよい。

【０００９】

【発明の実施の形態】

以下、この発明の実施例について説明する。

【００１０】

図１は、この発明の個人証明書発行システムの実施例を示しており、この図において、証明書発行センタ１０、協力会社サイト２０等がインターネット３０に接続されている。協力会社サイト２０は、構内ネットワーク網（ＬＡＮ）等によりイントラネットを構築されており、各イントラネットにクライアント端末２０１が接続されている。証明書発行センタ１０は、個人証明書発行に関連してイニシャティブをとる会社（幹事会社とも呼ぶ）またはインターネットサービスプロバイダ（ホスティングサービス）等に設けられるものである。ここでは、便宜上、証明書発行センタ１０は、幹事会社の社内に設けられているものとする。

【００１１】

この例において、証明書発行センタ１０は、協力会社サイト２０のクライアント端末２０１等からの個人証明書発行申請を受け取って発行処理を行うものである。

【００１２】

証明書発行センタ１０は、ウェブサーバ１０１、アプリケーションサーバ１０２、データベース管理システム１０３、メールサーバ１０４、クライアント端末１０５、ルータ１０６等を有している。これらコンピュータリソースはＬＡＮ１０７に接続されている。

【００１３】

ウェブサーバ１０１は、ＨＴＴＰ（ハイパーテキストトランスファプロトコル）プロトコルに従ってクライアント（クライアント端末２０１、１０５）から要求を受け取り、要求に応じたＨＴＭＬ文書（ＸＭＬ文書）をクライアントに転送する。アプリケーションサーバ１０２は、ウェブサーバ１０１を介してクライア

ントから送られたプログラム名および引数に基づいて種々の処理を実行するものである。アプリケーションサーバ１０２にかえてウェブサーバ１０１のＣＧＩ（コモンゲートインタフェース）のプログラムを用いてもよい。データベース管理システム１０３は、証明書発行に関連する種々のデータベースを管理するものである。データベースは、例えば、証明書データベース１０３ａ等である。

【００１４】

データベース管理システム１０３が管理する証明書データベース１０３ａに保持される証明書情報の簡略化した例を図２に示す。ここでは、証明書情報について説明する前に、この例で用いるＤＮ（ディスティングイシュトネーム、以下サブジェクト名とも呼ぶ。Ｘ．５０１）について説明しておく。この例では、サブジェクト名は、カントリネーム（Ｃ）、オーガニゼーションネーム（Ｏ）、第１オーガニゼーショナルユニットネーム（ＯＵ１）、第２オーガニゼーショナルユニットネーム（ＯＵ２）、第３オーガニゼーショナルユニットネーム（ＯＵ３）、コモンネーム（ＣＮ）により規定される。幹事会社以外の申請者に対してはＯＵ１として例えば「Ｐａｒｔｎｅｒ」等が記述される。幹事会社の社員については、ＯＵ１を省略したり、ＯＵ１として所定の部門名が記述される。ＯＵ２は、プロジェクト名が記述される。ただしプロジェクトと関係がない場合にはＯＵ２は省略される。ＯＵ３は、協力会社の会社名が記述される。もちろん、幹事会社の内部の者（社員等）に関してはＯＵ３は省略される。このようにして、サブジェクト名を用いてプロジェクトおよび協力会社を記述することができる。なお、ＯＵのサフィックスは、ＯＵの属性に対応して用いており、例えば部門（社外の組織）をあらわすＯＵ１は、部門の階層に応じてさらに階層的な構成を採用してもよい。例えば、「ｊｉｎｊｉ」（人事部）、「ｊｉｎｊｉ１」（第１人事課）等、ＯＵ１を複数規定できる。

【００１５】

なお、プロジェクトとは一括りに管理される業務や活動であり、ここでは便宜上、幹事会社と他の協力会社との間で行われる業務を指す。プロジェクトとの関連で協力会社が登録される。もちろん、幹事会社内のプロジェクトや非業務的な活動等を「プロジェクト」として扱ってもよい。このようにすることにより組織

構成から離れて証明書を発行することが可能となる。

【００１６】

サブジェクト名の具体例に説明する。

[Ｃ＝ＪＰ，Ｏ＝ＸＹＺ　Ｃｏ．，ＣＮ＝１２３４　Ｒｙｕ　Ｉｎａｄａ]

この例では、保持者がＸＹＺ株式会社の社員であり、社員番号が１２３４で、指名が「Ｒｙｕ　Ｉｎａｄａ」であることがわかる。

[Ｃ＝ＪＰ，Ｏ＝ＸＹＺ　Ｃｏ．，ＯＵ＝Ｐａｒｔｎｅｒ，ＯＵ＝Ｘｎｅｔ，ＯＵ＝ＡＢＣ　Ｃｏ．，ＣＮ＝１２３４　００１　Ｔａｒｏ　Ｆｕｊｉ]

この例では、保持者は協力会社のＡＢＣ株式会社の社員であり、プロジェクトＸｎｅｔに参画し、その業務目的が調達（コモンネームの００１が調達を意味する）であり、所属会社の社員番号が１２３４で、氏名が「Ｔａｒｏ　Ｆｕｊｉ」であることがわかる。

[Ｃ＝ＪＰ，Ｏ＝ＸＹＺ　Ｃｏ．，ＯＵ＝Ｐａｒｔｎｅｒ，ＯＵ＝Ｘｎｅｔ，ＣＮ＝１２３４　Ｈａｎａｋｏ　Ｆｕｊｉ]

この例では、保持者が派遣社員であり、その派遣社員番号が１２３４であり、氏名が「Ｈａｎａｋｏ　Ｆｕｊｉ」であることを示す。協力会社名あるいはプロジェクト名がないことから派遣社員と判断することができる。

【００１７】

図１の説明に戻る。データベース管理システム１０３が管理する証明書データベース１０３ａは、図２に示すように、証明書情報を保持している。図２に示すように、サブジェクト名は（Ｃ，Ｏ，ＯＵ１，ＯＵ２，ＯＵ３，ＣＮ）であり、コモンネームＣＮは、例えばＣＮ＝１２３４５　００１　Ｔａｒｏ　Ｙａｍａｄａである。「１２３４５」は協力会社ＡＢＣ内の一意の識別子例えば社員番号である。「００１」は幹事会社での業務の種別を示すＩＤである（例えば、調達業務、試作業務）。「ＴａｒｏＹａｍａｄａ]は申請者の氏名である。証明書データベース１１０は証明書ＩＤ、サブジェクト名（Ｃ，Ｏ，ＯＵ１，ＯＵ２，ＯＵ３，ＣＮ）、有効期限等を保持している。なお、証明書は、サブジェクト名、発行者名、公開鍵、発行者署名等を含むものである。

【００１８】

ウェブサーバ１０１、アプリケーションサーバ１０２、データベース管理システム１０３を用いて具体的な証明書発行処理の機能が実現される。クライアントはウェブベースで証明書発行システムの各種の機能を利用できる。

【００１９】

メールサーバ１０４はＳＭＴＰ（シンプルメールトランスファプロトコル）デーモン等を実行するものであり、メールの配送を行なう。

【００２０】

クライアント端末１０５は、ウェブブラウザを具備し、証明書発行システム内で証明書発行センタ１０のサービスの提供を受ける。

【００２１】

クライアント端末２０１は、協力会社サイト２０に配置されたパーソナルコンピュータ、ワークステーション等であり、ウェブブラウザを実装している。クライアント端末２０１は、証明書発行センタ１０が提供する証明書発行システムにアクセスし、雛型登録（会社登録）、個人証明書発行申請等を行なうことができる。証明書発行センタ１０はインターネット３０上に公開されているため、適宜ファイヤーウォール等のセキュリティ機構が設けられることが望ましい。

【００２２】

このような証明書発行センタ１０を用いて証明書の発行を申請し、申請が承認され、証明書が発行される。申請者は、証明書ＩＤを通知され、ウェブベースでこれを入力して証明書を取得する。

【００２３】

つぎに証明書を利用したアクセス制御について説明する。

【００２４】

図３はアクセス制御を行う機構を模式的に示すものである。この機構はウェブサーバ１０１、アプリケーションサーバ１０２等により実現される。図３において、セクセス制御機構は、認証部１５１、エレメント抽出部１５２、権限判別部１５３および権限登録部１５４等を含んで構成される。認証部１５１は図４に示すような認証手続をクライアント端末およびウェブサーバ１０１間で実現する。図４の認証手続は図から明らかであるのでとくに説明は行わない。認証部１５１

は、この認証手続の際に、クライアント端末から証明書を受け取る。この証明書は図４に示す認証手続に利用されるとともに、そのサブジェクト名がエレメント抽出部１５２に供給される。エレメント抽出部１５２はサブジェクト名の階層構造を辿って所定のエレメントを抽出する。この例では、ＯＵ１が「Ｐａｒｔｎｅｒ」であり、ＯＵ３に会社名がある場合に、ＯＵ２のプロジェクト名、ＯＵ３の会社名、ＣＮの業務種別コード（例えば「００１」）を抽出する。権限判別部１５３は図５に示すような区別に従って文書のアクセス権限を決定し、これをセッション番号に割り当てる。権限登録部１５４はセッション番号と権限との関係を登録する。以降、セッションが継続する間、このセッション番号に基づいてアクセス権限が許容される。

【００２５】

なお、以上の認証手続や権限制御は証明書発行センタ１０のウェブサーバ１０１との間でのみ可能なわけではなく、その他種々のサーバとの間で実行できることはもちろんである。

【００２６】

以上説明したようにこの発明によれば個人証明書のサブジェクト名を利用して簡易に保持者の権限や性質を判別でき、簡易にアクセス制御を行うことができる。

【００２７】

なお、この発明は上述の実施例に限定されるものではなくその趣旨を逸脱しない範囲で種々変更が可能である。例えば、上述例では、コモンネームに業務種別のコードを含ませたが、所定階層のオーガニゼーショナル・ユニット・ネームに含ませても良い。また、この発明のサブジェクト名の構成をアクセス制御以外の用途に用いることもできることは明らかである。

【００２８】

【発明の効果】

以上説明したように、この発明によれば、個人証明書を用いて簡易にアクセス制御等を行うことができる。

【図面の簡単な説明】

【図１】　この発明の実施例を全体として示すシステム図である。

【図２】　上述実施例の証明書データベースを説明する図である。

【図３】　上述実施例の申請者権限の制御を模式的に説明するブロック図である。

【図４】　上述実施例の認証手続を説明する図である。

【図５】　上述実施例の権限の区別を説明する図である。

【符号の説明】

１０　　証明書発行センタ

２０　　協力会社サイト

３０　　インターネット

１０１　　ウェブサーバ

１０２　　アプリケーションサーバ

１０３　　データベース管理システム

１０３ａ　　証明書データベース

１０４　　メールサーバ

１０５　　クライアント端末

１０６　　ルータ

１１０　　証明書データベース

１５１　　認証部

１５２　　エレメント抽出部

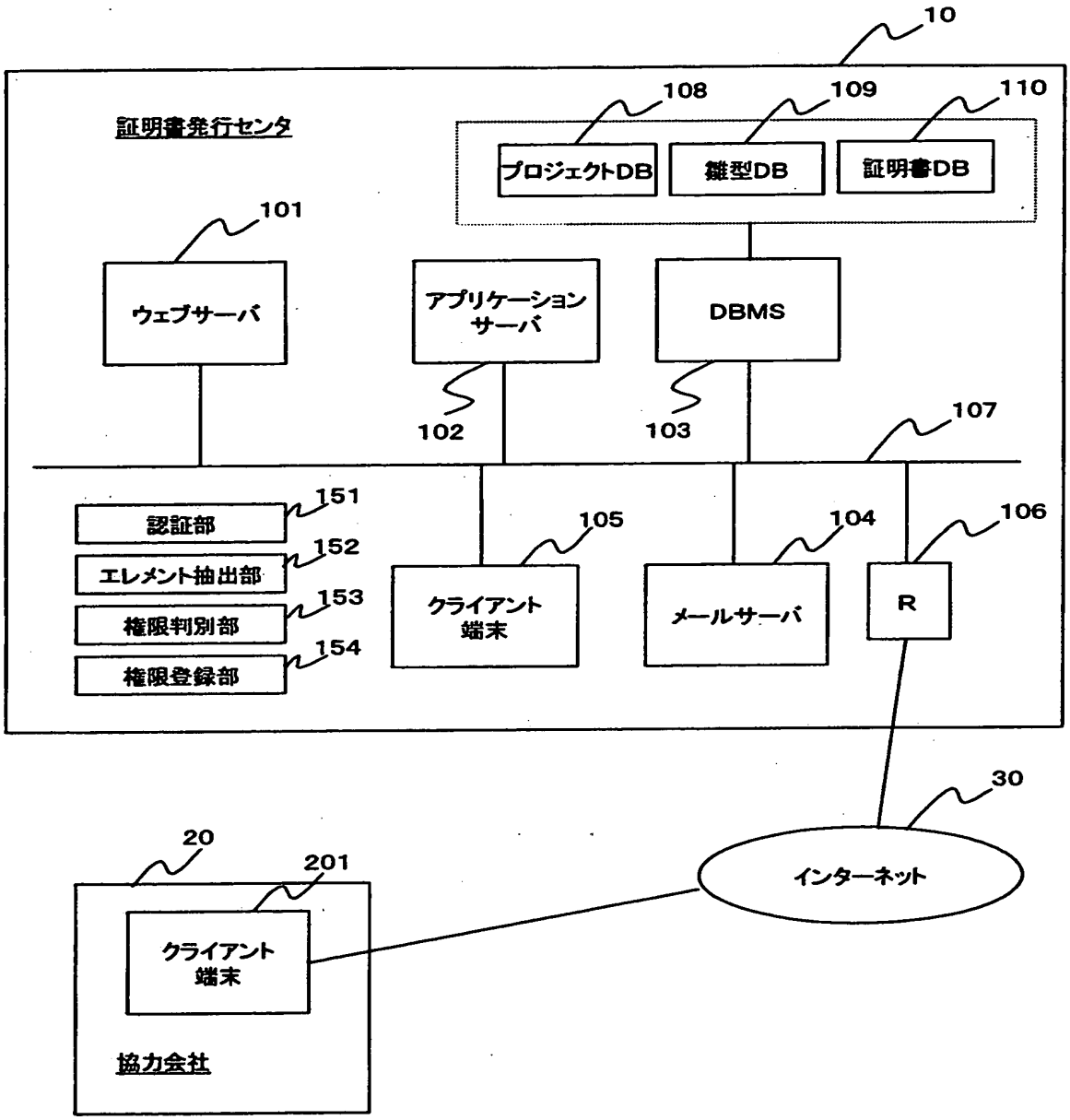
１５３　　権限判別部

１５４　　権限登録部

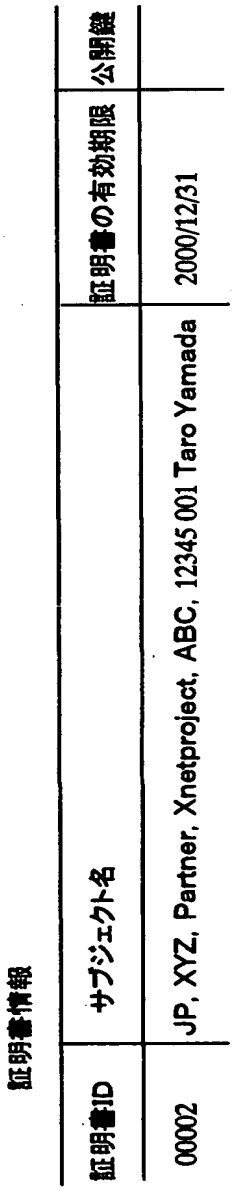
２０１　　クライアント端末

【書類名】　図面

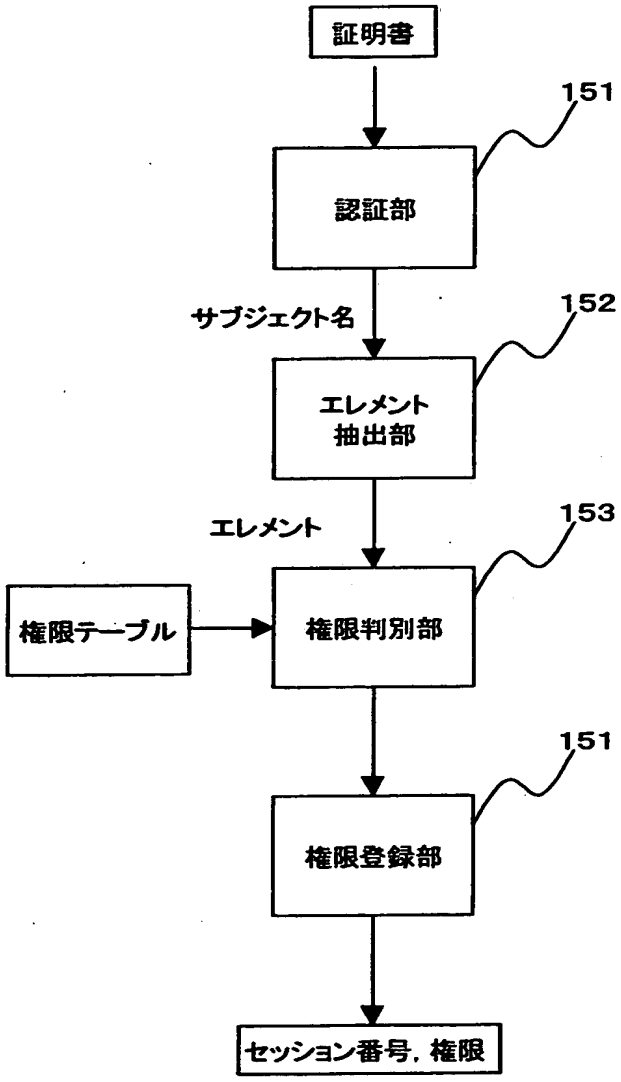
【図１】


10
証明書発行センタ
108
109
110
プロジェクトDB
雛型DB
証明書DB
101
ウェブサーバ
アプリケーション
サーバ
DBMS
102
103
107
認証部
151
エレメント抽出部
152
権限判別部
153
権限登録部
154
105
クライアント
端末
104
メールサーバ
106
R
30
インターネット
20
201
クライアント
端末
協力会社

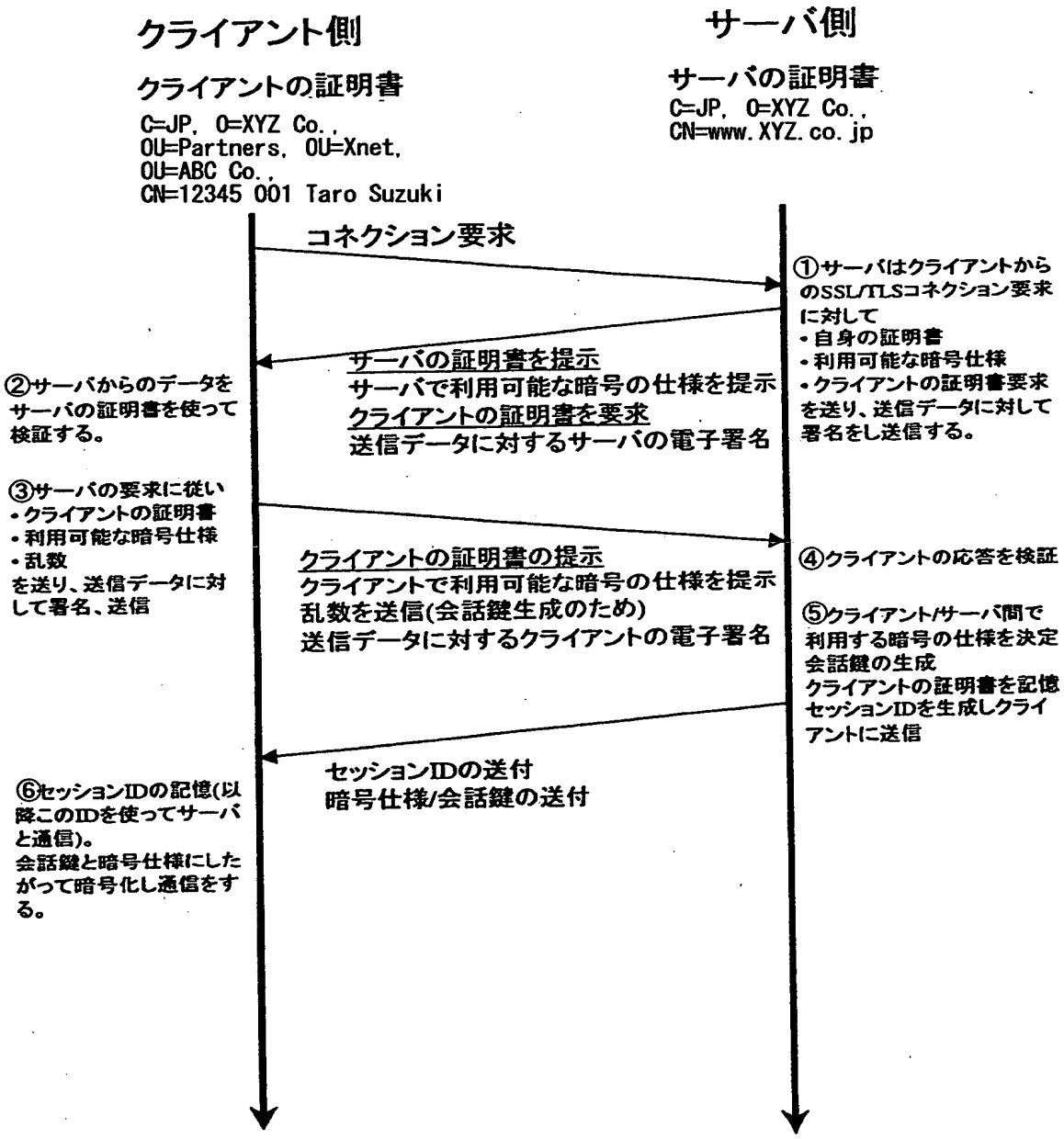
【図２】


証明書情報
証明書ID
サブジェクト名
証明書の有効期限
公開鍵
00002
JP, XYZ, Partner, Xnetproject, ABC, 12345 001 Taro Yamada
2000/12/31

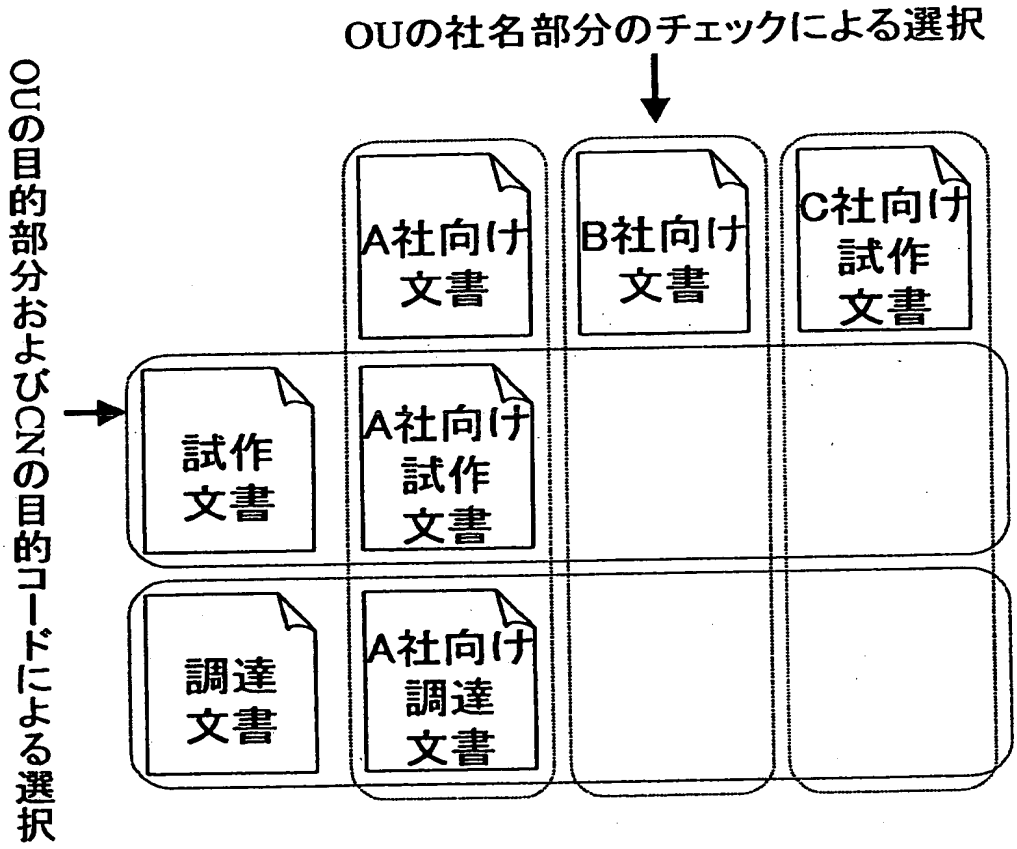
【図３】


証明書
151
認証部
サブジェクト名
152
エレメント
抽出部
エレメント
153
権限テーブル
権限判別部
151
権限登録部
セッション番号，権限

【図４】


クライアント側
クライアントの証明書
C=JP, O=XYZ Co.,
OU=Partners, OU=Xnet,
OU=ABC Co.,
CN=12345 001 Taro Suzuki
サーバ側
サーバの証明書
C=JP, O=XYZ Co.,
CN=www.XYZ.co.jp
コネクション要求
①サーバはクライアントからのSSL/TLSコネクション要求に対して
・自身の証明書
・利用可能な暗号仕様
・クライアントの証明書要求
を送り、送信データに対して署名をし送信する。
サーバの証明書を提示
サーバで利用可能な暗号の仕様を提示
クライアントの証明書を要求
送信データに対するサーバの電子署名
②サーバからのデータをサーバの証明書を使って検証する。
③サーバの要求に従い
・クライアントの証明書
・利用可能な暗号仕様
・乱数
を送り、送信データに対して署名、送信
クライアントの証明書の提示
クライアントで利用可能な暗号の仕様を提示
乱数を送信(会話鍵生成のため)
送信データに対するクライアントの電子署名
④クライアントの応答を検証
⑤クライアント/サーバ間で利用する暗号の仕様を決定
会話鍵の生成
クライアントの証明書を記憶
セッションIDを生成しクライアントに送信
セッションIDの送付
暗号仕様/会話鍵の送付
⑥セッションIDの記憶(以降このIDを使ってサーバと通信)。
会話鍵と暗号仕様にしたがって暗号化し通信をする。

【図５】


OUの社名部分のチェックによる選択
OCの目的部分およびCNの目的コードによる選択
A社向け文書
B社向け文書
C社向け試作文書
試作文書
A社向け試作文書
調達文書
A社向け調達文書

【書類名】　要約書

【要約】

【課題】　証明書のサブジェクト名を利用して簡易にアクセス制御等を行う。

【解決手段】　認証部１５１は認証手続をクライアント端末２０１およびウェブサーバ１０１間で実現する。認証部１５１は、この認証手続の際に、クライアント端末から証明書を受け取り、そのサブジェクト名がエレメント抽出部１５２に供給される。エレメント抽出部１５２はサブジェクト名の階層構造を辿って所定のエレメントを抽出する。権限判別部１５３は抽出したエレメントの種類、値に基づいて文書のアクセス権限を決定し、これをセッション番号に割り当てる。権限登録部１５４はセッション番号と権限との関係を登録し以降、セッションが継続する間、このセッション番号に基づいてアクセス権限が許容される。

【選択図】　図３

出　願　人　履　歴　情　報

識別番号　　〔０００００５４９６〕

１．変更年月日　　１９９６年　５月２９日
［変更理由］　住所変更
住　所　東京都港区赤坂二丁目１７番２２号
氏　名　富士ゼロックス株式会社